UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/676,474 | 09/30/2003 | Klimenty Vainstein | 2222.5450000 | 7534 |

26111 7590 09/04/2007

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.
1100 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

| EXAMINER | |
|---|---|
| PALIWAL, YOGESH | |
| **ART UNIT** | **PAPER NUMBER** |
| 2135 | |
| **MAIL DATE** | **DELIVERY MODE** |
| 09/04/2007 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/676,474 | VAINSTEIN ET AL. | |
| | Examiner | Art Unit | |
| | Yogesh Paliwal | 2135 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *18 June 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *18 June 2007* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

- Applicant's amendment filed on June 18,2007 has been entered. Applicant has amended claims 1-28. Currently claims 1-28 are pending in this application.
- Examiner acknowledges receiving a replacement sheet of drawings (Figure 3) with a revised Figure 3. The drawings were received on 6/18/2007. This drawing is acceptable. As a result, drawing objection is withdrawn.
- Examiner acknowledges clarification of claim language of claim 17 for minor informalities. As a result, all claim objections previously presented are withdrawn.
- Examiner acknowledges clarification of claim language of claims 27 and 28 for 35 U.S.C. 101 rejection. As a result, the 35 U.S.C. 101 rejection has been withdrawn for claims 27 and 28.

### *Claim Rejections - 35 USC § 101*

1. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

The USPTO "Interim Guidelines for Examination of Patent Applications for Patent Subject Matter Eligibility" (Official Gazette notice of 22 November 2005), Annex IV, reads as follows:

> In contrast, a claimed computer-readable medium encoded with a computer program is a computer element which defines structural and functional interrelationships between the computer program and the rest of the computer which permit the computer program's functionality to be realized, and is thus statutory. See Lowry, 32 F.3d at 1583-84, 32 USPQ2d at 1035.
>
> Claims that recite nothing but the physical characteristics of a form of energy, such as a frequency, voltage, or the strength of a magnetic field, define energy or magnetism, per se, and as such are nonstatutory natural phenomena. O'Reilly, 56 U.S. (15 How.) at 112-14. Moreover, it does not appear that a claim reciting a signal encoded with functional descriptive material falls within any of the categories of patentable subject matter set forth in Sec. 101.

... a signal does not fall within one of the four statutory classes of Sec. 101.

... signal claims are ineligible for patent protection because they do not fall within any of the four statutory classes of Sec. 101.

Claims **1-13** are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter as follows. Although Claims 1-13 are directed towards system of providing document security system, the specification provides intrinsic evidence that these claims are directed towards software alone. System as claimed in 1-13 is nothing more then software modules, which are capable of performing different tasks of the claimed system.

Claims 1-13 defines a system and method embodying functional descriptive material. However, the claims do not define a computer-readable medium or memory and is thus non-statutory for that reason (i.e., "When functional descriptive material is recorded on some computer-readable medium it becomes structurally and functionally interrelated to the medium and will be statutory in most cases since use of technology permits the function of the descriptive material to be realized" – Guidelines Annex IV). That is, the scope of the presently claimed system and method can range from paper on which the program is written, to a program simply contemplated and memorized by a person. The examiner suggests amending the claim to embody the program on "computer-readable storage medium" or equivalent in order to make the claim statutory. Any amendment to the claim should be commensurate with its corresponding disclosure. Also note that 35 U.S.C 101 requires that claimed invention, as a whole must produce a "useful, concrete and tangible result." State Street, 149 F.3d at 1373, 47 USPQ2d at 1601-02. When the system claim list only the software part, it would not

be able to produce any "useful, concrete and tangible result", in absence of corresponding hardware, as required by 35 U.S.C 101.

Examiner further would like to point out that just adding "computer-readable medium" will not be sufficient to make these claims statutory because the specification, at page 24 defines the computer readable medium as encompassing statutory media such as a "read-only memory", "random-access memory", "DC-ROMs", "DVDs", "magnetic tape", ""optical data storage devices", etc as well as ***non-statutory*** subject mater such as a "carrier waves" (which is a form of signal).

### *Claim Rejections - 35 USC § 102*

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims **1-9, 14-17 and 27** are rejected under 35 U.S.C. 102(e) as being anticipated by Bhide et al. (US 20040117371).

Regarding **Claim 1**, Bhide discloses:

A document security system for restricting access to secured documents **(Paragraph 0001 lines 1-2, "The invention relates the execution of event-based database access requests)** comprising:

at least one process-driven security policy that includes a plurality of states and transition rules, **(Figure 1, Numerals 20 and 18, Paragraph 0021 lines 1-3, "The event part 12 represents the condition that triggers the enforcement of the access control privileges specified in the access enforcement part 20 of the policy", Also at Paragraph 0003 lines 4-12, "In an event-based access control system, contingent access policies are used. Key to an event-based access control system is the idea of multiple states, Event triggers state transitions.")**

each of the states having associated therewith one or more access restrictions **(Paragraph 0025 lines 1-2, "The access enforcement part 20 represents the access control actions")** and the transition rules specifying circumstances under which the secured document is to transition from one state to another **(Paragraph 0023, lines 1-4, "The condition evaluation 16 defines the conditions that need to hold true after the event occurrence for the access enforcement 20 to be executed")**

an access manager that determines whether access to a secured document is permitted by a requestor based on the policy state associated therewith at the time access is requested and the corresponding one or more access restrictions thereof for the process-driven security policy **(Paragraph 0031 lines 3-10, "The Execution Model detects the occurrence of events. It also checks the truth-value of the conditions attached to the policies and depending on the truth-value, it executes the inference rules 18 as well as the access enforcement part 20 of the policy 10. The access Validation model 46, provides an interface to the end-user 52 to access data from the underlying databases or information repositories 54")**

Regarding **Claim 2,** the rejection of claim 1 is incorporated and further Bhide discloses that the one or more access restrictions for the secured document are automatically changed when the state of the process-driven security policy for the secured document changes. **(Paragraph 0025 lines 1-5, "The access enforcement part 20 represents the access control actions that are executed if an event occurs and the associated conditions evaluate to true)**

Regarding **Claim 3,** the rejection of claim 1 is incorporated and further Bhide discloses that events cause the state of the process-driven security policy for the secured document to automatically transition from one state to another **(Paragraph 0021 lines 1-4, "The event part 12 represents the condition that triggers the enforcement of the access control privileges", also at paragraph 0003, line 7, "Event triggers state transitions")**

Regarding **Claim 4**, the rejection of claim 3 is incorporated and further Bhide discloses that the events are internal or external events with respect to the document security system **(Paragraph 0021, lines 5-7, "Different kinds of events are supported including temporal events, database events and events external to the system")**

Regarding **Claim 5**, the rejection of claim 4 is incorporated and further Bhide discloses that at least one of the events is an external event from a document management system **(Paragraph 0021, lines 5-7, "Different kinds of events are supported including temporal events, database events and events external to the system")**

Regarding **Claim 6**, the rejection of claim 1 is incorporated and further Bhide discloses that one or more of the corresponding one or more access restrictions for access to the secured document remain intact when the state of the process-driven security policy for the secured document changes **(Paragraph 0103 lines 1-4, "whenever any entry is made in Leave Database automatically the above policy is executed and the access rights of the employee on confidential data are disabled") [access rights are remain intact so when leave flag clears and state changes, access rights can be restored]**

Regarding **Claim 7**, the rejection of claim 1 is incorporated and further Bhide discloses that events cause the state of the process-driven security policy to automatically transition from one state to another **(Paragraph 0021 lines 1-4, "The event part 12 represents the condition that triggers the enforcement of the access control privileges", also at paragraph 0003, line 7, "Event triggers state transitions")**

wherein the process-driven security policy includes at least a first state, a second state, and a third state, and wherein a first event causes transition from the first state to the second state, and a second event causes transition from the second state to a third state **(Paragraphs 0111, 0112, 0113, 0114)** *[Paragraph 0112 is the first state, paragraph 0113 is the second state and Paragraph 0114 is the third state, first event that causes transition from first to second state is "if the user has done business greater then $10,000" (paragraph 0113), and second event that causes transition from second to third state is "if the user has done business greater then $50,000 (paragraph 0114)"]*

Regarding **Claim 8**, the rejection of claim 1 is incorporated and further Bhide discloses that events cause the state of the process-driven security policy to automatically transition from one state to another **(Paragraph 0021 lines 1-4, "The event part 12 represents the condition that triggers the enforcement of the access control privileges", also at paragraph 0003, line 7, "Event triggers state transitions")**

wherein the process-driven security policy includes at least a first state and a second state, and wherein a first event causes transition from the first state to the second state. **(Paragraphs 0099, 0101 and 0103)** *[First state is when employee has access rights to confidential documents, second state is when employee does not have access rights to confidential documents, first event that causes transition from the first state to the second state is "When an employee goes on leave" (paragraph 0101)]*

Regarding **Claim 9**, the rejection of claim 1 is incorporated and further Bhide discloses that transition rules are based on events **(Paragraph 0023, lines 1-4, "The condition evaluation 16 defines the conditions that need to hold true after the event occurrence for the access enforcement 20 to be executed")**

Regarding **Claim 14**, Bhide discloses:

A method for transitioning at least one secured document through a security-policy state machine having a plurality of states **(Paragraph 0018 lines 1-4, "A method...for the execution of event-based access control with support for inference of access rights")**, comprising:

(a) receiving an event **(paragraph 0021 lines 1-5, "the event part 12...")**

(b) determining whether the event causes a state transition for the at least one secured document from a former state to a subsequent state of the security-policy state machine **(Paragraph 0024 lines 1-3, "The condition evaluation 16 defines the conditions that need to hold true after the event occurrence for the access enforcement 20 to be executed", at paragraph 0024 lines 1-3, "The access enforcement part represents the access control actions [states] that are executed if an event occurs and the associated conditions evaluate to true")**

(c) automatically transitioning from the former state to the subsequent state of the security-policy state machine when the determining (b) determines that the event causes the state transition **(Paragraph 0003 lines 4-12, "In an event-based access control system, contingent access policies are used. Key to an event-based access control system is the idea of multiple states, Event triggers state transitions.")**

Regarding **Claim 15**, the rejection of claim 14 is incorporated and Bhide further discloses that the security-policy state machine implements a process-driven security policy, wherein each state of the security-policy state machine has different access restrictions **(Page 2, table 2, column 4 "Access Enforcement", first access restriction is "Grant access to the stock...gold customer" and second access restriction is "If the parameter value > $1000 grant the user access...")**

Regarding **Claim 16**, the rejection of claim 14 is incorporated and Bhide further discloses each of the states of the security-policy state machine have different access

policies **(Page 2, table 2, column 4 "Access Enforcement", for first state, access policy is " access to the stock analysis data for the last six months " and for second state, access policy is "grant the user access to the stock analysis data for the last 1 month")**

Regarding **Claim 17**, the rejection of claim 16 is incorporated and further Bhide discloses that the security-policy state machine is provided as part of a document security system **(Paragraph 0030, line 3, "Definition and Deployment Model"),** and wherein the different access policies of the security-policy state machine are enforced by the document security system **(Paragraph 0031, lines1-3, "The definition and Deployment Model 42 is used for the definition of the access control policy 10 and its deployment as a component 48 within the database 50").**

Regarding **Claim 27**, Bhide discloses a computer readable medium including at least computer program code **(Paragraph 0018, line 1-2, "Computer program product")** which when executed by a computer, causes the computer to detect an occurrence of an event; determine whether the event causes a state transition for the at least one secured document from a former state to a subsequent state of a security-policy state machine having a plurality of states; and automatically transition from the former state to the subsequent state of the security-policy state machine upon determining that the event causes the state transition **(Rejected under the same rationale as claim 14)**

***Claim Rejections - 35 USC § 103***

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

**Claim 10** is rejected under 35 U.S.C. 103(a) as being unpatentable over Bhide et al. (US 2004/0117371) in view of Smith et al. (US 2003/0217333).

Regarding **Claim 10**, the rejection of claim 9 is incorporated. Bhide does not teach that the transition rules are written in XML.

However, Smith et al. in the same field of endeavor of network security discloses that rules are written in XML **(paragraph 0032, line 2, "rules may be written in an XML format")**

Therefor, it would have been obvious at the time the invention was made to one of ordinary skill in the art to write the transition rules of Bhide in XML as taught by Smith because *"XML schemas may be parsed in real-time, allowing for the real-time modification of the rules"* **(Smith, paragraph 0032, lines 4-6)**

Claims **11-13 and 18-20** are rejected under 35 U.S.C. 103(a) as being unpatentable over Bhide et al. (US 2004/0117371) in view of Dilkie et al. (US 6341164).

Regarding **Claim 11**, the rejection of claim 1 is incorporated and Bhide further discloses that events cause the state of the process-driven security policy for the

secured document to transition from a previous state to a current state **(Paragraph 0021 lines 1-4, "The event part 12 represents the condition that triggers the enforcement of the access control privileges", also at paragraph 0003, line 7, "Event triggers state transitions")**

Bhide does not teach that the secured document is modified when the process-driven security policy for the secured document transitions from the previous state to the current state.

However, Dilkie in the same field of endeavor of data security systems discloses modifying the secured document **(Column 3 lines 24-25, "...re-encrypts the encrypted data with a different encryption process...")**

Therefore, it would have been obvious at the time the invention was made to one of ordinary skill in the art to modify the secured document as taught by Dilkie when the security policy for the secured document transitions from the previous state to the current state as taught by Bhide to *"re-encrypt the encrypted data with a different encryption process in response to detected improper encryption key usage"* **(Dilkie, Column 3 lines 24-25)**

Regarding **Claim 12**, the rejection of claim 11 is incorporated and Dilkie further discloses that the secured document includes at least a security information portion **(Column 3, lines 62-63, "The cryptographic key package information is preferably contained as header data")** and an encrypted data portion **(column 4, lines 7-8, "the encrypted message data with the header data")** information portion including at least an encrypted key **(Column 4 lines 1-3, "A cryptographic key package may include,**

**for example, a symmetric encryption key wrapped, or encrypted, with an asymmetric encryption key, such as a recipient's public key...")**, and the key being encrypted must be decrypted in order to decrypt the encrypted data portion **(Column 7 lines 46-50, "The corresponding private key (for example, signing key) is used to unwrap the cryptographic key package to recover a message encryption key as known in the art. The system may re-encrypt the key package with a different asymmetric key and/or algorithm as shown in block 409. The analyzer 103 may then decrypt the message data in any suitable manner using the message encryption key as shown in block 410".)**

The combination as applied in above rejection of claim 11, does not teach that when the process-driven security policy for the secured document transitions from the previous state to the current state, the secured document is modified by decrypting the encrypted key and then re-encrypting the key, whereby the key is encrypted differently for the current state than the previous state.

However Dilkie, in the same reference further discloses that the secured document is modified by decrypting the encrypted key and then re-encrypting the key, whereby the key is encrypted differently for the current state than the previous state **(column 8, lines 11-18, "incoming message is encrypted under algorithm X with symmetric key Y wrapped (encrypted) with asymmetric key Z, the system may decrypt asymmetrically to recover the symmetric key Y, and re-encrypt the symmetric key Y with a different asymmetric key Z' and replace the previous**

**cryptographic key package with the new re-encrypted key data forming a new cryptographic key package in the header")**

Therefore, it would have been obvious at the time the invention was made to one of ordinary skill in the art to modify the secured document by decrypting the encrypted key and then re-encrypting the key as taught by Dilkie when document transit from one state to another state as taught by Bhide to re-encrypt the *"header without re-encrypting the file itself, thereby only changing the wrapping on the header key"* **(Dilkie, column 8, lines 19-21)**

Regarding **Claim 13**, the rejection of claim 11 is incorporated and further Bhide discloses that when permitted, access to the secured document is available at a client machine (Paragraph 0031, lines 8-10, "**The access Validation model 46, provides an interface to the end-user 52 to access data from the underlying databases or information repositories 54")**

Regarding **Claim 18**, the rejection of claim 14 in incorporated. Bhide does not teach modifying the secured document to reflect the subsequent state of the security-policy state machine.

However, Dilkie in the same field of endeavor of data security systems discloses modifying the secured document **(Column 3 lines 24-25, "...re-encrypts the encrypted data with a different encryption process...")**

Therefore, it would have been obvious at the time the invention was made to one of ordinary skill in the art to modify the secured document as taught by Dilkie when the security policy for the secured document transitions from the previous state to the

current state as taught by Bhide to *"re-encrypt the encrypted data with a different encryption process in response to detected improper encryption key usage"* **(Column 3 lines 24-25)**

Regarding **Claim 19**, the rejection of claim 14 is incorporated. Bhide does not teach retrieving an encrypted file key from the secured document; decrypting, when permitted by the former state of the security-policy state machine, the encrypted file key to yield a file key; subsequently encrypting the file key in accordance with the subsequent state of the security-policy state machine; and storing the secured document, the secured document including at least an encrypted data portion and the subsequently encrypted file key.

However, Dilkie discloses a method of retrieving an encrypted file key from the secured document; decrypting, when permitted by the former state of the security-policy state machine, the encrypted file key to yield a file key; subsequently encrypting the file key in accordance with the subsequent state of the security-policy state machine; and storing the secured document, **(column 8, lines 11-18, "incoming message is encrypted under algorithm X with symmetric key Y wrapped (encrypted) with asymmetric key Z, the system may decrypt asymmetrically to recover the symmetric key Y, and re-encrypt the symmetric key Y with a different asymmetric key Z' and replace the previous cryptographic key package with the new re-encrypted key data forming a new cryptographic key package in the header. The message data with the new cryptographic key package may then be stored")** the secured document including at least an encrypted data portion **(column 4, lines 7-8,**

**"the encrypted message data with the header data")** and the subsequently encrypted file key **(Column 3, lines 62-63, "The cryptographic key package information is preferably contained as header data")**

Therefore, it would have been obvious at the time the invention was made to one of ordinary skill in the art to modify the secured document by decrypting the encrypted key and then re-encrypting the key as taught by Dilkie when document transit from one state to another state as taught by Bhide to re-encrypt the *"header without re-encrypting the file itself, thereby only changing the wrapping on the header key"* **(Dilkie, column 8, lines 19-21)**

Regarding **Claim 20**, the rejection of claim 14 is incorporated. Bhide does not teach a method of retrieving an encrypted file key from the secured document; obtaining a private state key associated with the former state of the security-policy state machine; decrypting the encrypted file key using the private file key; obtaining a public state key associated with the subsequent state of the security-policy state machine; subsequently encrypting the file key in accordance with the public state key; and storing the secured document, the secured document including at least an encrypted data portion and the subsequently encrypted file key.

However, Dilkie discloses a method of retrieving an encrypted file key from the secured document; obtaining a private state key associated with the former state of the security-policy state machine; decrypting the encrypted file key using the private file key; obtaining a public state key associated with the subsequent state of the security-policy state machine; subsequently encrypting the file key in accordance with the public

state key; and storing the secured document, **(column 8, lines 11-18, "incoming message is encrypted under algorithm X with symmetric key Y wrapped (encrypted) with asymmetric key Z, the system may decrypt asymmetrically to recover the symmetric key Y, and re-encrypt the symmetric key Y with a different asymmetric key Z' and replace the previous cryptographic key package with the new re-encrypted key data forming a new cryptographic key package in the header. The message data with the new cryptographic key package may then be stored")** the secured document including at least an encrypted data portion **(column 4, lines 7-8, "the encrypted message data with the header data")** and the subsequently encrypted file key **(Column 3, lines 62-63, "The cryptographic key package information is preferably contained as header data")**

Therefore, it would have been obvious at the time the invention was made to one of ordinary skill in the art to modify the secured document by decrypting the encrypted key and then re-encrypting the key as taught by Dilkie when document transit from one state to another state as taught by Bhide to re-encrypt the *"header without re-encrypting the file itself, thereby only changing the wrapping on the header key"* **(column 8, lines 19-21)**

Claims **21-26** are rejected under 35 U.S.C. 103(a) as being unpatentable over Bhide et al. (US 2004/0117371) in view of Moriconi et al. (US 6941472), and further in view of DeTreville (US 2004/0098580).

Regarding **Claim 21**, Bhide discloses a method for imposing access restrictions on electronic documents, comprising:

providing at least one process-driven security policy **(Figure 1, Numeral 20, Paragraph 0021 lines 1-3, "access control privileges specified in the access enforcement part 20 of the policy")** at a server machine **(Paragraph 0030, line 1, "A database system")**

the process-driven security policy having a plurality of states associated therewith, each of the states having distinct access restrictions **(Paragraph 0003 lines 4-12, "In an event-based access control system, contingent access policies are used. Key to an event-based access control system is the idea of multiple states, Event triggers state transitions.")**

transitioning the process-driven security policy from one state to a current state **(Paragraph 0021 lines 1-4, "The event part 12 represents the condition that triggers the enforcement of the access control privileges", also at paragraph 0003, line 7, "Event triggers state transitions")**

and subsequently determining at the server computer whether a requestor is permitted to access the electronic document, the access being based on a current state of the process-driven security policy **(Paragraph 0031 lines 3-10, "The Execution Model detects the occurrence of events. It also checks the truth-value of the conditions attached to the policies and depending on the truth-value, it executes the inference rules 18 as well as the access enforcement part 20 of the policy 10.**

**The access Validation model 46, provides an interface to the end-user 52 to access data from the underlying databases or information repositories 54")**

Bhide does not teach providing a reference to the process-driven security policy at a client machine, the reference referring to the process-driven security policy resident on the server machine; associating the reference to an electronic document

However, Moriconi in the same field of endeavor of secure distribution system disclosed a method of providing a reference to the process-driven security policy at a client machine, the reference referring to the process-driven security policy resident on the server machine **(Column 5, lines 22-24, "A policy manager located on a server for managing and distributing a policy to a client")** associating the reference to an electronic document **(Column 5, lines 24-26, "an application guard located on the client, the application guard acting to grant or deny access to various components of the client, as specified by the policy")**

Therefore, it would have been obvious at the time the invention was made to one of ordinary skill in the art to provide a reference to the client machine, as taught by Moriconi, of the process-driven security policy, as taught by Bhide so that *"central policy server automatically distributes (over the network) only the relevant portion of the enterprise policy to each remote service"* **(Moriconi, Column 4, lines 12-14)**

The combination of Bhide and Moriconi does not teach that the current state being informed to the server computer by sending the reference to the server computer.

However, Detreville in the same field of endeavor of digital rights management system, discloses that the current state being informed to the server computer by

sending the reference to the server computer **(Paragraph 0024, lines 1-4, "When analyzing license 304, access control module 316 may request current state information from state server 310. In response to this request, state server 310 may transmit current state information 320 to access control module 316")**

Therefore, it would have been obvious at the time the invention was made to one of ordinary skill in the art to send a reference of the current state information about the document, as taught by Detreville, to the authentication server as taught by Bhide to *" evaluate whether one or more conditions included in license 304 have been satisfied"* (Detreville, Paragraph 0024, lines 6-7).

Regarding **Claim 22**, the rejection of claim 21 is incorporated and further Bhide discloses that transitioning is automatically performed based on events **(Paragraph 0021 lines 1-4, "The event part 12 represents the condition that triggers the enforcement of the access control privileges", also at paragraph 0003, line 7, "Event triggers state transitions")**

Regarding **Claim 23**, the rejection of claim 21 is incorporated and further Bhide discloses that transitioning is performed at the server machine. **(Paragraph 0030, "A database system...three parts- the definition and deployment part 42, the execution model 44 and the access validation model 46", Paragraph 0031, lines 6-8, "...depending on the truth-value, it executes the inference rules 18 as well as the access enforcement part 20 of the policy 10")**

Regarding **Claim 24**, the rejection of claim 21 is incorporated and further Moriconi discloses that associating associates the reference to a group of documents

**(Column 5, lines 24-26, "an application guard located on the client, the application guard acting to grant or deny access to various components [group of documents] of the client, as specified by the policy")**

Regarding **Claim 25**, the rejection of claim 21 is incorporated and further Moriconi discloses that method pertains to a group of electronic documents, and wherein all of the electronic documents of the group are always in the same state of the process-driven security policy **(Column 5, lines 24-26, "an application guard located on the client, the application guard acting to grant or deny access to various components [group of documents] of the client, as specified by the policy") [at any given time client receive only relevant portion of the enterprise policy and applies it to various components within the client, then all components of client at any given time uses the same policy and thus are in same state]**

Regarding **Claim 26**, the rejection of claim 21 is incorporated and further Bhide discloses that determining comprises evaluating the process-driven security policy of an electronic document at the server computer based on at least the security policy restrictions for the current state of the process-driven security policy for the electronic document **(Paragraph 0031 lines 3-10, "The Execution Model detects the occurrence of events. It also checks the truth-value of the conditions attached to the policies and depending on the truth-value, it executes the inference rules 18 as well as the access enforcement part 20 of the policy 10. The access Validation model 46, provides an interface to the end-user 52 to access data from the underlying databases or information repositories 54")**

Regarding **Claim 28**, claim 28 is "computer readable medium" claim analogous to "method" claim 21. Claim 28 is rejected based on the same rationale as the rejection of claim 21.

***Response to Arguments***

***Rejections under 35 U.S.C 101:***

- Please note that rejection of claims 14-20 has been withdrawn. However, rejection were withdrawn by examiner after realizing that interim guidelines recite that "a claimed computer-readable medium encoded with a computer program is a computer element which defines structural and functional interrelationships between the computer program and the rest of the computer which permit the computer program's functionality to be realized, and is thus statutory". In case of method claims having only software code performing different task, it is noted that for the software to be able to realize the functionality of the computer program, hardware is inherently present. However, such is not the case with system claims where only the components of the systems are listed and no claim of functionality being realized is present. As a result if system is only listing the software part of the system, hardware cannot be assumed to be present unlike the method claims because simply listing the components of the system does not result in functionality being realized. Also note that 35 U.S.C 101 requires that claimed invention as a whole must produce a "useful, concrete and tangible

result." State Street, 149 F.3d at 1373, 47 USPQ2d at 1601-02. When the system claim list only the software part, it would not be able to produce any "useful, concrete and tangible result", in absence of corresponding hardware, as required by 35 U.S.C 101.

- Applicant argues that: "On page 4 of the Office Action, the Examiner concedes that claims 1-20 are directed to systems and methods, but asserts that Applicants' specification "provides intrinsic evidence that these claims are directed towards software alone." The Examiner seems to have misunderstood embodiments in Applicants' specification and what is claimed in claims 1-20. Paragraphs 11-20 and 36-47 of Applicants' specification provide support for the document security systems and methods claimed in claims 1-20."
- In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

**Rejections under 35 U.S.C 102:**

**Claims 1-9:**

Applicant had following arguments regarding the novelty of claim 1 when comparing to the reference(s) used in rejection in the last office action:

- Applicant argues that: "Bhide infers database access privileges for access requests when no explicit privileges exist (Bhide, paragraph [0009], lns. 1-3) and lacks any teaching of transition rules for secured documents."
- Examiner respectfully disagree and still maintain that Bhide reference discloses transition rules for secured document (at Paragraph 0023, lines 1-4, "The condition evaluation 16 defines the conditions that need to host true after the event occurrence for the access enforcement 20 to be executed"), also from paragraph 0026 and corresponding table 1 bellow paragraph 0026, it can be seen that access to the database [secure document] can be restricted based on a combination of condition evaluation and inference rule, in other words when the customer requesting access is a "gold type and the total transaction amount done by the user within last 2 months is greater then $10,000", customer gets access to six months data, however when user is not type "gold" but the transaction value is greater then $1000, only 1 month data is available to the user. So the amount of data [secured document] from the database changes to 1 month data and 6 month data based on these "condition evaluation" and "Inference rule" can be interpreted as secure document transitioning from one state (1st state can be data of last 1 month, and the second state can be data of last 6 months) to other because of "condition evaluation" and "Inference rule", which in combination can be interpreted as a transition rules. Also at paragraph 0003 lines 4-12, Bhide discloses, "In an event-based access control system, contingent access policies are used. Key to an event-based access control

system is the idea of multiple states, Event triggers state transitions". Therefore, Bhide clearly teaches this claimed limitation.

- Applicant further argues that: "Bhide does not teach or suggest securing or encrypting documents based upon process-driven security policy states that have specified access restrictions and transition rules as recited in Applicants' claim 1."
- In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., "securing or encrypting document based upon process-driven security policy states") are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).
- Applicant further argues that: "Applicants are unable to find any teaching in Bhide of a document security system that protects files, executable code, or images. Applicants are also unable to identify any teaching in Bhide of a document security system that protects secured files with keys or encryption as recited in claim 1 and disclosed in Applicants' specification."
- Once again, In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., "protects files, executable code, or images" and "protects secured files with keys or encryption") are not recited in the rejected claim(s).

Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See In re Van Geuns, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

- Applicant further argues that: "Bhide does not teach use of an access manager to determine a requestor's access to secured documents as recited in claim 1."
- Examiner respectfully disagree and still maintain that Bhide discloses an access manager (Paragraph 0031 lines 3-10, "The Execution Model detects the occurrence of events. It also checks the truth- value of the conditions attached to the policies and depending on the truth-value, it executes the inference rules 18 as well as the access enforcement part 20 of the policy 10. The access Validation model 46 provides an interface to the end-user 52 to access data from the underlying databases or information repositories 54"). Bhide's "Execution model" and "The access Validation model" in combination can be interpreted as an access manager with determines whether access to a secured document is permitted by a requestor based on the state and the corresponding one or more access restrictions. Therefore, Bhide clearly teaches this claimed limitation.

Note: Examiner has traversed all the arguments presented by applicant regarding the patentability of claim 1 and still maintains that claim 1 (as previously presented) is anticipated by Bhide reference. Applicant presented no arguments for claims 2-9; as a result, Bhide also anticipates claims 2-9 (as previously presented) for the same reasons presented in the last office action.

**Claims 14-17**

Applicant had following arguments regarding the novelty of claim 14 when comparing to the reference(s) used in rejection in the last office action:

- Applicant argues that: "Applicants have examined paragraphs 3, 18, 21, and 24 of Bhide and are unable to find any teaching of transitioning a secured document through a security policy state machine as recited in claim 14".
- Examiner respectfully disagree and still maintain that Bhide reference discloses transitioning a secured document through a security policy state machine (at Paragraph 0023, lines 1-4, "The condition evaluation 16 defines the conditions that need to host true after the event occurrence for the access enforcement 20 to be executed"), also from paragraph 0026 and corresponding table 1 bellow paragraph 0026, it can be seen that access to the database [secure document] can be restricted based on a combination of condition evaluation and inference rule, in other words when the customer requesting access is a "gold type and the total transaction amount done by the user within last 2 months is greater then $10,000", customer gets access to six months data, however when user is not type "gold" but the transaction value is greater then $1000, only 1 month data is available to the user. So the amount of data [secured document] from the database changes to 1 month data and 6 month data based on these "condition evaluation" and "Inference rule" can be interpreted as secure document transitioning from one state (1st state can be data of last 1 month, and the second state can be data of last 6 months) to other because of "condition

evaluation" and "Inference rule", which in combination can be interpreted as a transition rules. Also at paragraph 0003 lines 4-12, Bhide discloses, "In an event-based access control system, contingent access policies are used. Key to an event-based access control system is the idea of multiple states, Event triggers state transitions". Therefore, Bhide clearly teaches this claimed limitation.

- Applicant further argues that: "Bhide also lacks claim 14's recited step of automatically transitioning a secured document's state from a former state to a subsequent state in a security-policy state machine when an event causes a state transition... and Bhide does not automatically transition a document's security state based on events as recited in claim 14."
- Examiner respectfully disagree and still maintain that Bhide reference discloses automatically transitioning a secured document's state from a former state to a subsequent state in a security-policy state machine when an event causes a state transition (Paragraph 0003 lines 4-12, "In an event-based access control system, contingent access policies are used. Key to an event-based access control system is the idea of multiple states, Event triggers state transitions."). Also at paragraph 0103 "whenever any entry is made in the Leave Database automatically the above policy is executed and the access rights of the employee on confidential data are disabled." In this situation confidential data being available to particular employee when his name is not in leave database can be interpreted as 1$^{st}$ state of the secured document and confidential data [secured document] being disable for that employee when his name is in leave database

can be interpreted as a 2nd state. "...automatically the above policy is executed and the access rights of the employee on confidential data are disabled", can be interpreted as automatically transitioning a secured document's state from a former state (1st state) to a subsequent state (2nd state) and, "whenever any entry is made in the Leave Database"; can be interpreted as event causing the transition. Therefore, Bhide clearly teaches this claimed limitation.

Note: Examiner has traversed all the arguments presented by applicant regarding the patentability of claim 14 and still maintains that claim 14 (as previously presented) is anticipated by Bhide reference. Applicant presented no arguments for claims 15-17; as a result, Bhide also anticipates claims 15-17 (as previously presented) for the same reasons presented in the last office action.

**Claim 27:**

Applicant had following arguments regarding the novelty of claim 27 when comparing to the reference(s) used in rejection in the last office action:

- Applicant argues that: "Applicants are unable to identify any disclosure in Bhide of computer code that automatically transitions a secured document from a former security state to a subsequent state in a security-policy state machine as recited in claim 27."
- Examiner respectfully disagree and would like to point out that Bhide reference discloses automatically transitioning a secured document's state from a former state to a subsequent state in a security-policy state machine when an event

causes a state transition (Refer to examiner's remark above for the similar limitation in claim 14). And at Paragraph 0018 Bhide discloses a Computer Program Product "for execution of event-based access control with support of inference of access rights". Examiner assert that it is implied that step of "automatically transitioning a secured document's state from a former state to a subsequent state in a security-policy state machine when an event causes a state transition" is done by a computer code and not done manually because Bhide discloses a computer program product which performs all the method step using the hardware in the overall system.

- Applicant further argues that: "As disclosed in paragraph 42 of Applicants' specification, access to secured documents recited in claim 27 is provided through encryption and access rules. Applicants are unable to find any teaching in Bhide of a computer readable medium with program code that protects files, executable code, or images. Applicants are also unable to identify any teaching in Bhide of a computer readable medium with computer code that protects secured files with keys or encryption as recited in claim 27 and disclosed in Applicants' specification."
- Once again, In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., "protects files, executable code, or images" and "protects secured files with keys or encryption") are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from

the specification are not read into the claims. See In re Van Geuns, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Note: Examiner has traversed all the arguments presented by applicant regarding the patentability of claim 21 and still maintains that claim 21 (as previously presented) is anticipated by Bhide reference.

**Rejections under 35 U.S.C 102:**

**Claim 10:**

Applicant had following arguments regarding the novelty of claim 10 when comparing to the reference(s) used in rejection in the last office action:

- Applicant argues that: "Smith does not teach or disclose a file or document security system with transition rules written in XML that specify when a secured document transitions from one state to another as recited in Applicants' claim 10."
- This argument is not considered persuasive since only the concept of writing rules in XML format is taken from the Smith reference and combined with Bhide. Smith does not have to disclose a file or document security system with transition rules that specify when a secured document transitions from one state to another because these limitation are disclosed by Bhide. Smith reference is used to teach the concept of writing rules in XML format as a secondary teaching for the motivation(s) provided. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking

references individually where the rejections are based on combinations of references. See In re Keller, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); In re Merck & Co., 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

Note: Examiner has traversed all the arguments presented by applicant regarding the patentability of claim 10 and still maintains that claim 10 (as previously presented) is unpatentable over Bhide reference in view of Smith Reference.

**Claim 11-13:**

Applicant had following arguments regarding the novelty of claim 11 when comparing to the reference(s) used in rejection in the last office action:

- Applicant argues that: Dilkie does not teach or suggest modifying a secured document based on a security policy state transition as recited in claim 11. Dilkie discloses re-encryption of files when the wrong encryption key was used to encrypt data (Dilkie, col. 3, lns. 23-27), but does not suggest modifying secured documents based on a process-driven security policy change as recited in Applicants' claim 11.
- This argument is not considered persuasive since only the concept of modifying the document is taken from Dilkie reference and Bhide discloses security policy state transition as established above. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations

of references. See In re Keller, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); In re Merck & Co., 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

Note: Examiner has traversed all the arguments presented by applicant regarding the patentability of claim 11 and still maintains that claim 11 (as previously presented) unpatentable over Bhide reference in view of Dilkie. Applicant presented no arguments for claims 12 and 13; as a result, Bhide in view of Dilkie also make claims 12-13 (as previously presented) unpatentable for the same reasons presented in the last office action.

**Claims 18-20:**

- Applicant argues that: "The applied references alone or in combination do not teach or suggest modifying a secured document to reflect a subsequent state of a security-policy state machine as recited in claim 18".
- In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, Examiner relied on Column 3 lines 24-25 of Dilkie to provide motivation to combine and further would like to clarify why a person of ordinary

skill in the art would have done the same if he had knowledge of both references. Dilkie at Column 3 lines 24-25 discloses "re-encrypt the encrypted data with a different encryption process in response to detected improper encryption key usage". The fact that applicant has recognized another advantage which would flow naturally from following the suggestion of the prior art cannot be the basis for patentability when the differences would otherwise be obvious. See *Ex parte Obiaya*, 227 USPQ 58, 60 (Bd. Pat. App. & Inter. 1985).

- Applicant further argues that: "Dilkie's "apparatus and method for facilitating an encryption process" discloses re-encrypting data with a different encryption process when an improper encryption key is detected (Dilkie, col. 3, lns. 14-15 and lns. 23-27), but clearly does not teach modifying a secured document based on security policy state transitions as recited in claim 18."
- In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).
- Regarding Claim 19 applicant argues that: "Although Dilkie may disclose deleting unnecessary header cryptographic key packages, compressing message data, obtaining the decryption key, decrypting message data, compressing data, and then re-encrypting the compressed data (Dilkie, col. 8, lns. 4-10); compression and encryption of data does not suggest encrypting a secured document's key in

accordance with a subsequent state of a security-policy state machine as recited in claim 19."

- In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See In re Keller, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); In re Merck & Co., 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).
- Regarding Claim 20 applicant argues that: Although Dilkie may disclose obtaining a message's decryption key, decrypting message data, compressing data, and then re-encrypting the compressed data (Dilkie, col. 8, lns. 4-10), compression and encryption of data does not teach or suggest encrypting a secured document's file key in accordance with the corresponding public state key as recited in claim 20.
- Examiner respectfully disagree and would like to point out that at Column 8, lines 11-18, Dilkie discloses "...asymmetric key Z [public key of previous state], the system may decrypt symmetrically to recover the symmetric key Y, and re-encrypt the symmetric key Y with a different asymmetric key Z' [public key of new state] and replace the previous cryptographic key package with the...", this re-encrypting of key y with different asymmetric (public) key can be interpreted as encrypting a secured document's file key in accordance with the corresponding public state key as required by claim 20.

- Regarding Claim 20, applicant further argues that: "The Examiner's piecemeal assembly of parts of Bhide and Dilkie to cure the deficiencies in Bhide destroys the teaching of both of these references by making the systems/methods of operation unsatisfactory for their intended purposes and/or changing the systems/principles of operation".
- In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

Note: Examiner has traversed all the arguments presented by applicant regarding the patentability of claims 18-20 and still maintains that claims 18-20 (as previously presented) are unpatentable over Bhide reference in view of Dilkie.

**Claims 21-26:**

- Applicant argues that: "Although Moriconi may disclose a system for managing computer system security requirements with a policy manager on a server that manages and distributes a global security policy to clients (Moriconi, col. 5, lns. 19-26), Moriconi does not suggest providing references to clients for a process-driven security policy with a plurality of states as recited in claim 21."
- In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the

rejections are based on combinations of references. See In re Keller, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); In re Merck & Co., 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

- Applicant further argues that: "Applicants have examined lines 1-4 of paragraph 24 of DeTreville and are unable to identify a teaching of a client informing a server of a process-driven security policy state with distinct access restrictions as recited in claim 21."
- Once again, in response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See In re Keller, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); In re Merck & Co., 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).
- Applicant further argues that: "The Examiner's piecemeal assembly of parts of Bhide, Moriconi, and DeTreville to cure the deficiencies in Bhide destroys the teaching of both of these references by making the systems/methods of operation unsatisfactory for their intended purposes and/or changing the systems/principles of operation."
- In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See In re Keller, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); In re Merck & Co., 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

Note: Examiner has traversed all the arguments presented by applicant regarding the patentability of claim 21 and still maintains that claim 21 (as previously presented) is unpatentable over Bhide reference in view of Moriconi and further in view of DeTreville. Applicant presented no arguments for claims 22-26; as a result, Bhide in view of Moriconi and further in view of DeTreville also make claims 22-26 (as previously presented) unpatentable for the same reasons presented in the last office action.

***Conclusion***

4. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Yogesh Paliwal whose telephone number is (571) 270-1807. The examiner can normally be reached on M-F: 7:30 AM - 5:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

YP
8/23/2007

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100